Forensics Laptop Hardening Guide

Target System: Windows 10 Pro

Inhalt

Protection And Hardening

W10Privacy

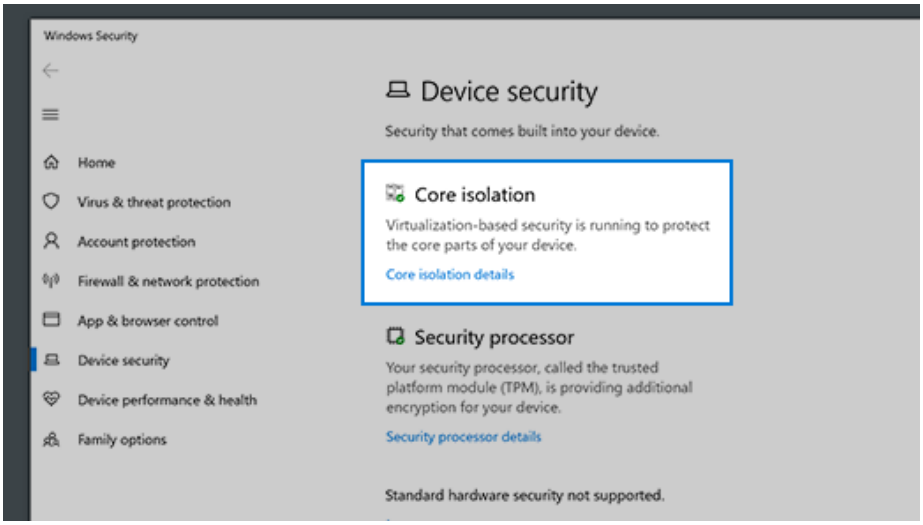
Siehe Ordner „W10Privacy“ – CSIRT oder OWN Patch

Device protection in Windows Security

Quelle: https://support.microsoft.com/en-us/windows/device-protection-in-windows-security-afa11526-de57-b1c5-599f-3a4c6a61c5e2

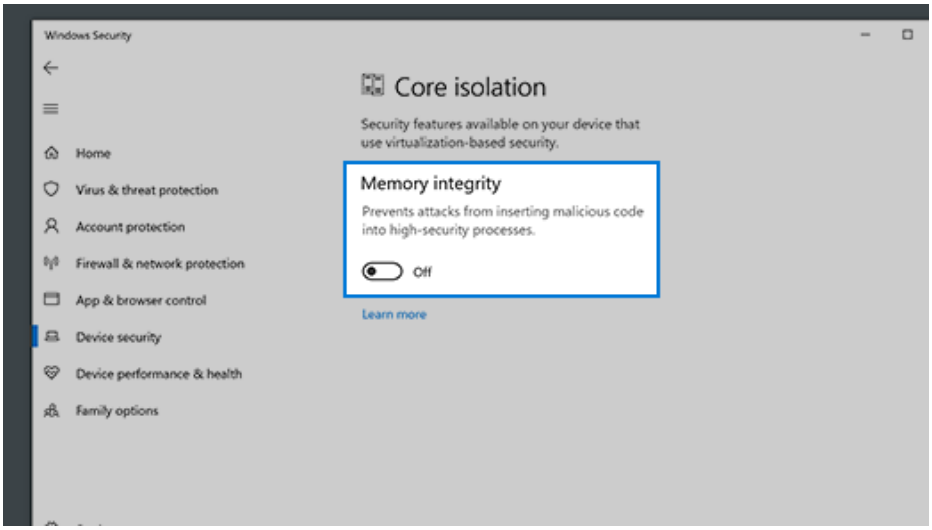
Core isolation

Core isolation provides added protection against malware and other attacks by isolating computer processes from your operating system and device. Select Core isolation details to enable, disable, and change the settings for core isolation features.



Memory integrity

Memory integrity is a feature of core isolation. By turning on the Memory integrity setting, you can help prevent malicious code from accessing high-security processes in the event of an attack.

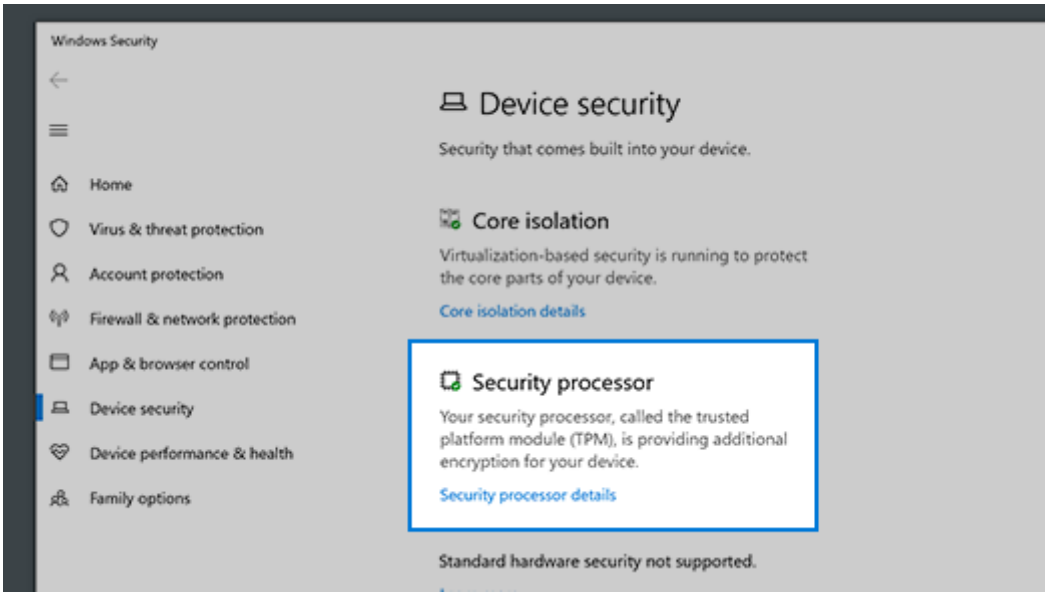


To learn more about Core Isolation and memory integrity see https://support.microsoft.com/en-us/windows/core-isolation-e30ed737-17d8-42f3-a2a9-87521df09b78

Security processor

Your security processor provides additional encryption for your device.

Security processor details



This is where you'll find info about the security processor manufacturer and version numbers, as well as about the security processor's status. Select Security processor details for additional info and options.

Note: If you don't see a Security processor entry on this screen then it's likely that your device doesn't have the TPM (Trusted Platform Module) hardware necessary for this feature or that it's not enabled in UEFI (Unified Extensible Firmware Interface). Check with your device manufacturer to see if your device supports TPM and, if so, steps to enable it.

If your security processor isn't working properly, you can select the Security processor troubleshooting link to see any error messages and advanced options. For more information see: Security Processor troubleshooting.

Secure boot

Secure boot prevents a sophisticated and dangerous type of malware—a rootkit—from loading when you start your device. Rootkits use the same permissions as the operating system and start before it, which means they can completely hide themselves. Rootkits are often part of an entire suite of malware that can bypass local logins, record passwords and keystrokes, transfer private files, and capture cryptographic data.

You may have to disable secure boot to run some PC graphics cards, hardware, or operating systems such as Linux or earlier versions of Windows. For more info, see How to disable and re-enable secure boot.

Hardware security capability

At the bottom of the Device security screen, one of the following messages appears, indicating the security capability of your device.

Your device meets the requirements for standard hardware security

This means your device supports memory integrity and core isolation and also has:

- TPM 2.0 (also referred to as your security processor)
- Secure boot enabled
- DEP
- UEFI MAT

Your device meets the requirements for enhanced hardware security

- This means that in addition to meeting all the requirements of standard hardware security, your device also has memory integrity turned on.

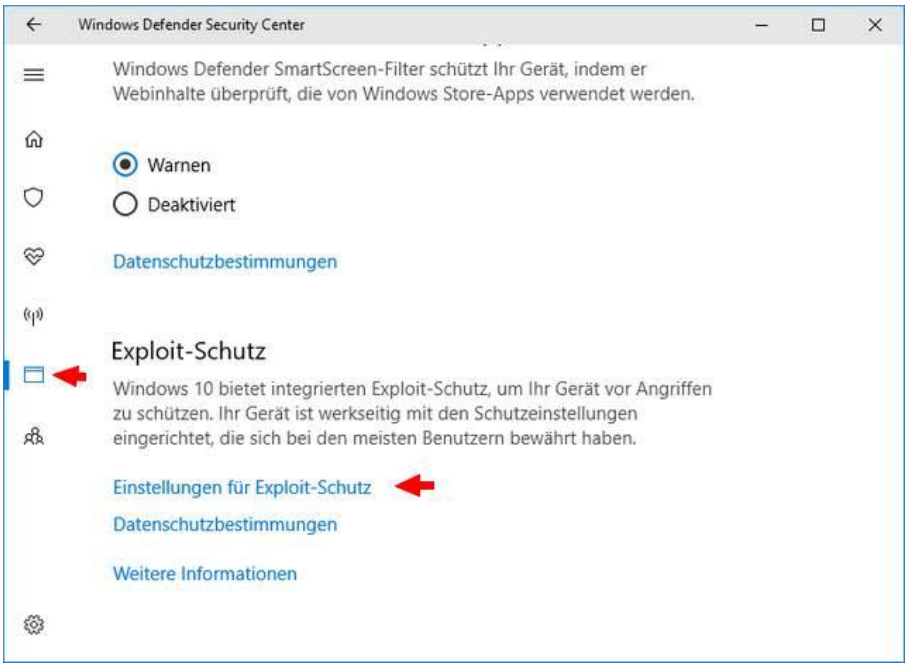
Your device has all Secured-core PC features enabled

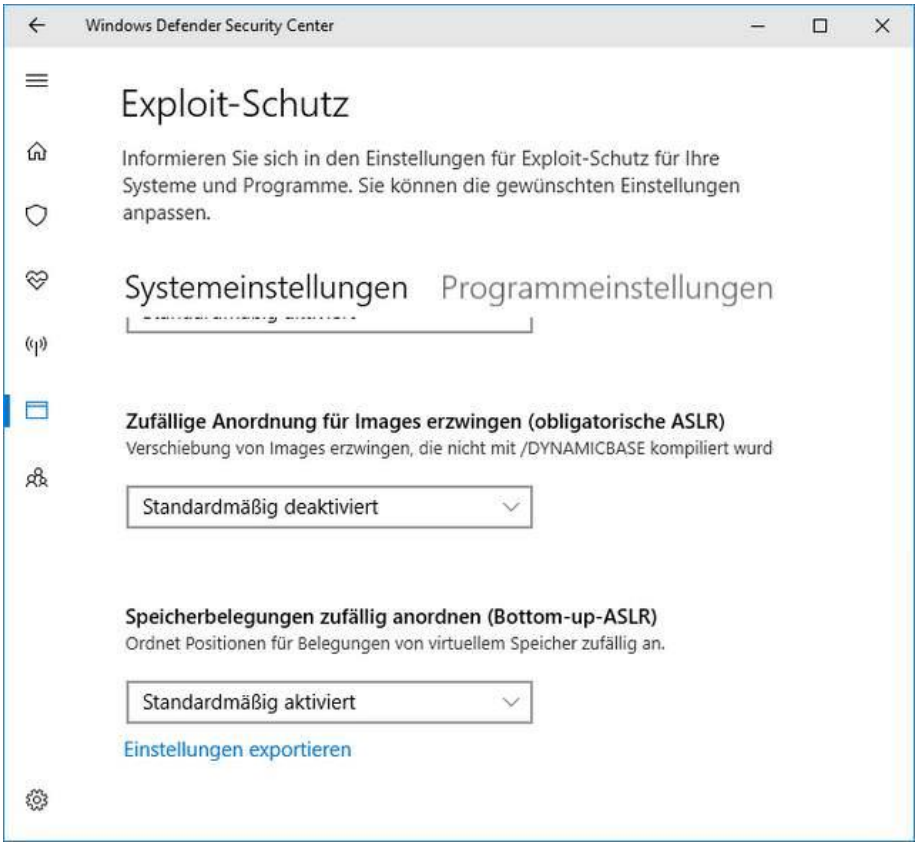
- Note: Prior to Windows 20H2 this message said "Your device exceeds the requirements for enhanced hardware security".
- This means that in addition to meeting all the requirements of enhanced hardware security, your device also has System Management Mode (SMM) protection turned on.

Standard hardware security not supported

- This means that your device does not meet at least one of the requirements of standard hardware security.
- Improving hardware security
    - If the security capability of your device isn't what you'd like it to be, you might need to turn on certain hardware features (such as secure boot, if supported) or change the settings in your system's BIOS. Contact your hardware manufacturer to see what features are supported by your hardware and how to activate them.

Activate / Check ASLR-Protection





Quelle 2: https://www.hysolate.com/learn/os-isolation/windows-hardening-checklist-for-windows-server-windows-10/

Windows User Configuration (optional for Forensic Laptop)

Follow these guidelines to reduce risks from privileged user accounts on Windows Server:

- Disable the local administrator—it is usually not required, and is a popular target for attackers.
- Set up a custom local account in the administrators group
- Prefer to run as a regular user account—to reduce the chance of account compromise and when you need to perform operations that require administrative privileges, request elevation using "Run As" (the Windows equivalent of sudo).

Leverage Built-In Windows 10 Security Tools

Enterprise editions of Windows 10 come with several built-in security tools, including:

- Windows Defender Advanced Threat Protection – an advanced security system that includes state of the art antimalware protection, as well as exploit protection, automated attack surface reduction, application control, and hardware-based isolation.
- Microsoft SmartScreen – scans downloads and blocks execution of malicious payloads.
- Windows Sandbox – lets users install untrusted applications in a secure, isolated environment.

In addition to these built-in Microsoft tools, assess your threat environment and deploy additional antivirus or endpoint protection tools on all protected Windows 10 machines.

Application Management (optional for Forensic Laptop)

It is strongly preferred to configure Windows to only allow the installation of approved applications from controlled software repositories or application marketplaces. You can do this by setting the "Allow apps from the Store only" option under Apps & Features, or using Windows Defender code Integrity policies.

This can prevent attackers from emailing malware to users, convincing them to download and install malware, or deploying malware via drive-by downloads or deceptive links on malicious websites. Note that even if you require administrative access on the local machine to install software, attackers can bypass this with social engineering.

Application Control (optional for Forensic Laptop)

Many attack vectors rely on execution of malicious code, even if it is not installed on the user's device. Whitelisting and blacklisting of executables in Windows 10 can be effective at preventing these attacks. Many security best practices advise creating a new whitelist of files that are allowed to execute on end-user machines, without relying on lists from application vendors or existing files on the machine.

However, in real enterprise environments, it can be difficult to create such a whitelist and maintain it across a large number of machines. Whitelists will also tend to be overly restrictive, hurting user productivity.

Disable Remote Access

Windows 10 comes with Microsoft Remote Desktop that provides remote access to a user's machine. This feature is often used by attackers to gain remote control of user devices, install malware, and steal information. Remote Desktop is disabled by default, but in case users enable it, it is important to make sure it is disabled except when needed for approved, legitimate use.

Tip: https://carbidesecure.com/resources/how-to-disable-remote-access-in-windows-10/

PowerShell

PowerShell is a scripting language that is extremely powerful in the hands of an attacker. Follow these guidelines to secure systems against PowerShell exploits:

- Remove PowerShell version 2.0 or earlier, which had security vulnerabilities
  - Check with: `Get-Host | Select-Object Version`
- Set PowerShell to Constrained Language Mode
  - https://support.alertlogic.com/hc/en-us/articles/4410220960795-Enable-Windows-PowerShell-Logging
- Enable PowerShell logging to provide an audit trail
- Setting an execution policy – a safety feature that specifies under which conditions PowerShell will load configuration files and run scripts

Enable Auto-Updates

Deploy Microsoft security updates on all user devices immediately. Automate and enforce deployment of regular Windows updates—if possible, without the user's involvement.

Support for Windows 7 ended in January 2020, and so any end-user device running Windows 7 or earlier is at immediate risk of cyberattacks. If users are running an older version of Windows that is no longer supported, upgrade it to a supported version urgently, and in cases where upgrades are not possible, isolate the outdated systems from the network.

Learn more in our detailed guide to Windows 10 hardening

Quelle 3: https://resources.infosecinstitute.com/topic/windows-10-hardening-techniques/

Clean up unwanted programs

Even in fresh installations of Windows 10, a system likely has unnecessary programs installed. These programs expand the attack surface and become potential points of entry for attackers. Installed programs should be reviewed then the unneeded deleted. Verify that all installed programs are legitimate and not pirated software, which could be filled with bloat and malware

Encryption

Hard drives should be encrypted. Windows 10 comes with BitLocker as its built-in encryption solution and the encryption process is easy. Trusted Platform Module (TPM) must be enabled to encrypt with BitLocker. Later editions of Windows 10 come with TPM enabled by default, making it one less thing to think about.

Secure boot should be used in conjunction with encryption. It will link the hard drive to the system hardware and ensure that only Microsoft-trusted firmware is used upon boot.

Enable the guards!

Windows 10 has several built-in security solutions for different aspects of the OS that use "guard" as their feature surname. Below is a list of "guards" that should be enabled to reduce attack surface.

- Device Guard
- Credential Guard
    - https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage
- Application Guard
- Exploit Guard

Ransomware protection

Windows Defender offers ransomware protection, but it's not turned on by default. During the hardening process look in Virus & Threat Protection → Ransomware protection → Manage ransomware protection. Make sure that controlled folder access is on. Keep in mind that this will prevent applications from creating files within the documents folder.

Secure authentication

Authentication needs to be hardened as it can be a glaring expanse of attack surface. The best way to do this is to set multi-factor authentication. This can include a complex password as one of the factors, with the other either being a PIN, gesture, biometrics or picture password.

Secure web browsing

Edge is Windows 10's default browser and it is also an app. This means that it can operate in a sandbox if needed, giving it some heightened security.

Quelle 4: https://www.hysolate.com/learn/os-isolation/windows-10-hardening-19-ways-to-secure-your-workstations/

Windows Defender Device Guard

Windows Defender Device Guard is designed to protect your device by whitelisting applications and implementing a code integrity policy. This prevents malicious code from finding its way onto your computer and compromising the operating system.

Code integrity policies determine if software is allowed to run on Windows 10, so IT can block unknown or untrusted plug-ins, applications and add-ons from accessing endpoint devices.

Windows Defender Application Guard

Windows Defender Application Guard is built into Microsoft Edge to protect the desktop from malicious activity. This security tool runs browser sessions in a virtual machine (VM) to isolate them from the desktop.

Trusted sites can be whitelisted so they don't have to run Windows Defender Application Guard, but any other site accessed must open with this tool. The site is run in an isolated Hyper-V container.

Windows Defender Credential Guard

Windows Defender Credential Guard helps prevent credential theft by isolating login information from the overall operating system.

With Credential Guard, user credentials can only be accessed by privileged software. To prevent brute-force attacks, credential information is stored as randomized, full-length hashes. Domain credentials are also protected.

Tip: https://carbidesecure.com/resources/how-to-check-for-viruses-using-built-in-tools-in-windows-10/

Microsoft SmartScreen

SmartScreen is a built-in feature that scans and prevents the execution of known malware. It also compares the reliability of emails and websites to Microsoft's blacklist, so it can alert Windows 10 users when they try to open suspicious content. Combined with traditional cybersecurity awareness training for employees, this cloud-based tool can provide an additional level of protection against phishing and malware attacks.

Windows Hello

Microsoft Windows Hello is an access control feature that supports biometric identification via fingerprint scanners, iris scanners, and facial recognition technologies on compatible devices running Windows 10. The Hello engine allows users to securely log into a device with the necessary hardware components so they don't have to enter a password.

Enhanced Mitigation Experience Toolkit and Exploit Protection

Enhanced Mitigation Experience Toolkit (EMET) is a security tool designed by Microsoft to provide protection and mitigation for third-party and legacy applications. In Windows 10 versions, from 1709 and onwards, as well as Windows Server version 2016 and onwards, EMET comes as part of the exploit protection function of the operating system.

Windows Information Protection

As more organizations allow employees to use their personally-owned devices, the risk of accidental data leaks increases. Employees use many corporate applications and services that cannot be controlled by the organization. Emails, public cloud services, and social media platforms, for example, can all lead to data leaks.

Windows Information Protection (WIP) is designed to protect against potential data leaks without disrupting user experience. Formerly known as enterprise data protection (EDP), this service is especially designed to reduce data leak risks originating from bring your own device (BYOD) practices, including protection for both personally-owned and company-owned devices.

WIP does not require modifying existing environments. It is offered as a mobile application management (MAM) mechanism on Windows 10. You can use WIP to manage data policy enforcement for documents and applications on Windows 10 desktop operating systems. It can also help you remove access to company data from all devices.

WIP can help separate personal and company data without making employees switch between applications or environments. The service also provides data protection for existing line-of-business applications without having to update the applications. Additionally, it lets you wipe company data from enrolled Intune MDM devices without having to delete personal data.

Another major advantage of WIP is that it provides audit reports that let you track issues as well as remedial actions. You can integrate WIP with existing management systems, including Microsoft Endpoint Configuration Manager and Microsoft Intune. It can also be integrated with existing MDM systems, which can help you set up, deploy, and manage WIP.

Enable File Backups (Optional)

Setting up file backups on a regular basis can help prevent critical data loss during disasters like hardware failures or malware attacks. To help you protect your data, Windows 10 offers several tools and features, including:

- Use File History – this free tool can help you easily backup files.
- Create recovery drives – serve as backup images from which you can restore a system.

For Forensic Cases: Backup Cases after and while working on them

Quelle 5: https://carbidesecure.com/resources/security-best-practices-hardening-windows-10/#auto-login

Disable Windows 10 automatic login

This is one of the first settings that you should change or check on your computer.

When you first set up a new PC with Windows 10, you create a user account. By default, your new account is set to log in automatically at startup. If you're at home all the time or don't have access to any sensitive data, then this might not be a problem. But it can create a serious security risk if anyone can open your computer, then immediately get access to your data and company systems. This is especially important if you travel with a laptop, bringing it with you to places like a coffee shop, airport, or open co-working spaces.

Depending on the security policies at your company, this may also be something your employer requires.

It is easy to disable, so in only a few steps, you can turn off auto-login. Get the steps here: How to Disable Automatic Login in Windows 10

Bonus tip: If you do travel with your laptop or work from public places, you may want to get a privacy screen protector. Those can make the screen look dark to keep a criminal from "shoulder surfing"

and seeing your private information. Privacy screens can also reduce glare and make the screen easier on your eyes, another reason to get one.

Set a password with your screensaver.

There's no reason someone in your office, home, or travel location should be able to access your system if you step away for a few minutes. It's a good idea to make sure your PC automatically locks after a set period of inactivity.

While it's actually a security setting, you'll find it inside the "Appearances and Personalization" section within your Control Panel. You can turn this on when you adjust your screensaver settings. It's easy to choose the time until a screensaver displays, set the screen saver, and turn on the setting that brings you back to the login screen when you come back.

Security starts with following the most basic protocols. So make sure you password protect your PC.

Get the steps for password protecting your PC after a screensaver here: How to Set a Windows Screen Saver Password

Turn on your firewall.

In recent versions of Windows operating systems, including Windows 10, your firewall is enabled by default. Easy enough! You're probably all set here. But it doesn't hurt to check your settings to make sure your firewall wasn't turned off.

Windows Firewall is a built-in network security system. It's designed to prevent unauthorized access to or from your private network.

Network firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet would pass through the firewall, which examines each message and blocks any that don't meet the specified security criteria.

If you want to check the settings for your Windows Firewall, we have instructions for you here: How to Turn on the Firewall in Windows 10

Set up a password manager.

If you frequently forget the email you used to sign up for an account or your password, you'll LOVE using a password manager.

Windows 10 and your browser may have some features for saving passwords, but a best practice in the infosec world is to use a dedicated password manager. It's like upgrading from a tiny safe in your house to a vault in a world-class bank.

Password managers have you create a master password for your "vault" of sensitive accounts and login information. The best ones sync can automatically add new passwords, sync with your phone and computer, generate and autofill strong passwords, and let you share a specific password with coworkers or friends.

Use: KeePass 2 Locally!